

離散関数の複雑性に関する考察

工学部 情報システム工学科 3 年 039 番
田中 諒

2007 年 2 月 12 日

主に暗号を研究対象とする分野では、一部から全体を推測することが出来ないような性質（すなわちランダムな性質）を持つ写像（暗号化関数）は、重要な意味を持つ。しかしながら、特に有限の定義域を持つ写像に対して、はたしてそれが上のような性質を持つのかどうか、それを計測する方法として特に有効なものは余り知られていない。

今回の私の研究では、有限集合の中で、特に整数を法とする剰余類を定義域及び値域とする写像のランダムさ（乱雑さ）または複雑さを定量的に与える手法について提案を行い、また、その数学的性質と有効性についての検証の結果をまとめた。

また、その手法を用いて既存の暗号方式の暗号化関数の複雑さを調べ、その安全性を評価した。

1 関数の乱雑さの指標—Cosmoness—の提案

複雑さの指標として、以下のような量—Cosmoness—を定義した。

$$\text{Cosm}(f) := “ f \text{ のパワースペクトルの分散 } ” \quad (1.1)$$

定性的な考察によって、 $\text{Cosm}(f)$ は、関数 f がランダムなときに小さい実数となることが確認できた。

2 Cosmoness の性質

定量的な評価によって、理想的にランダムな関数 f に対しては、 $\text{Cosm}(f)$ は 1 となることを実験から推測し、また、証明を行った。また、 $\text{Cosm}(f)$ が最大となることと、 f が 1 次関数であることは必要十分条件であることも証明した。

3 Cosmoness を用いた暗号化関数の評価

既存の暗号方式の暗号化関数に対して、その Cosmoness を計算し、直感的な複雑さとの対比を行った。その結果、大変良い結果が得られた。

また、例外的に良い対応が得られないような関数の存在が予想されたが、そのような関数はほとんど見つからなかった。

4 今後の方針・課題

Cosmoness の定義の細分化、Cosmoness という量へのさらに慎重な意味づけ、Cosmoness を求めるときの計算量の改善などを今後の課題とした。

以上